In the Claims

This listing of claims will replace all prior versions, and listings of claims in the application. Applicant has submitted a new complete claim set showing marked up claims with insertions indicated by underlining and deletions indicated by strikeouts and/or double bracketing. Please amend claims 1-5, 7, 11, and 17 as indicated below. No new matter has been added.

1. (Currently Amended) A method for a first computing device to make authentication information available to a second computing device, the method comprising:

creating authentication information, the authentication information including content data, a public key of the first computing device, a network address of the first computing device usable to route a message to the first computing device, and a digital signature, the network address having a portion derived from the public key of the first computing device, the digital signature generated by signing with a private key of the first computing device corresponding to the public key, the digital signature generated from ~~at least one of~~ the content data and/or a hash value of data including the content data; and

making the authentication information available to the second computing device, in part by sending a message to the second computing device, the message including the digital signature in a packet option and including the network address.

2. (Currently Amended) A computer-readable medium containing instructions for performing a method for a first computing device to make authentication information available to a second computing device, the method comprising:
creating authentication information, the authentication information including content data, a public key of the first computing device, a network address of the first computing device usable to route a message to the first computing device, and a digital signature, the network address having a portion derived from the public key of the first computing device, the digital signature generated by signing with a private key of the first computing device corresponding to the public key, the digital signature generated from ~~at least one of~~ the content data and/or a hash value of data including the content data; and
making the authentication information available to the second computing device, in part by sending a message to the second computing device, the message including the digital signature in a packet option and including the network address.

3. (Currently Amended) A method for a second computing device to authenticate content data made available by a first computing device, the method comprising:
accessing authentication information made available by the first computing device, the authentication information including the content data, a public key of the first computing device, a first network address of the first computing device, and a digital signature, the first network address being usable to route a message to the first computing device;
deriving a portion of a second network address from the public key of the first computing device;

validating the digital signature by using the public key of the first computing device; and

accepting the content data if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from at least one of the content data and/or a hash value of data including the content data,

wherein the second computing device accesses the public key of the first computing device over an insecure channel, and wherein if the content data are not accepted, then the public key is discarded.

4. (Currently Amended) The method of claim 3 wherein the second computing device accesses the public key of the first computing device over an insecure channel to a device including ~~at least one of~~ the first computing device and/or a key publishing device.

5. (Currently Amended) A computer-readable medium containing instructions for performing a method for a second computing device to authenticate content data made available by a first computing device, the method comprising:

accessing authentication information made available by the first computing device, the authentication information including the content data, a public key of the first computing device, a first network address of the first computing device, and a digital signature, the first network address being usable to route a message to the first computing device;

deriving a portion of a second network address from the public key of the first computing device;

validating the digital signature by using the public key of the first computing device; and

accepting the content data if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from ~~at least one of~~ the content data and/or a hash value of data including the content data,

wherein the second computing device accesses the public key of the first computing device over an insecure channel, and wherein if the content data are not accepted, then the public key is discarded.

6. (Currently Amended) A method for a computing device to derive a node-selectable portion of a network address from a public key of the computing device, the network address being usable to route a message to the computing device, the method comprising:

hashing the public key;

comparing a portion of a value produced by the hashing with a portion of the network address other than the node-selectable portion, the portion of the network address other than the node selectable portion being defined by a network address protocol;

if the portions do not match, choosing a modifier, appending the modifier to the public key, and repeating the hashing and comparing; and

if the portions match, setting the node-selectable portion of the network address to a portion of the value produced by the hashing.

7. (Currently Amended) The method of claim 6 wherein the portion of the network address other than the node-selectable portion comprises an element including ~~at least one of~~ a "u" bit, a "g" bit, and/or a portion of a route prefix.

8. (Currently Amended) A computer-readable medium containing instructions for performing a method for a computing device to derive a node-selectable portion of a network address from a public key of the computing device, the method comprising:

hashing the public key;

comparing a portion of a value produced by the hashing with a portion of the network address other than the node-selectable portion, the portion of the network address other than the node selectable portion being defined by a network address protocol;

if the portions do not match, choosing a modifier, appending the modifier to the public key, and repeating the hashing and comparing; and

if the portions match, setting the node-selectable portion of the network address to a portion of the value produced by the hashing.

9. (Currently Amended) A method for a computing device to derive a node-selectable portion of a network address from a public key of the computing device and from a route prefix of the network address of the computing device, the method comprising:

hashing the public key and at least a portion of the route prefix of the network address, the route prefix being suitable for routing a message to an appropriate link in a network;

setting the node-selectable portion of the network address to a portion of the value produced by the hashing;

checking to see if the network address as set is already in use; and

if the network address as set is already in use, choosing a modifier, appending the modifier to the public key, and repeating the hashing, setting, and checking.

10. (Currently Amended) A computer-readable medium containing instructions for performing a method for a computing device to derive a node-selectable portion of a network address from a public key of the computing device and from a route prefix of the network address of the computing device, the method comprising:

hashing the public key and at least a portion of the route prefix of the network address, the route prefix being suitable for routing a message to an appropriate link in a network;

setting the node-selectable portion of the network address to a portion of the value produced by the hashing;

checking to see if the network address as set is already in use; and

if the network address as set is already in use, choosing a modifier, appending the modifier to the public key, and repeating the hashing, setting, and checking.

11. (Currently Amended) A method for a second computing device to maintain a cache of at least one public key/network address association, the method comprising:

accessing authentication information made available by a first computing device, the authentication information including content data, a public key of the first computing device, a first network address of the first computing device usable to route a message to the first computing device, and a digital signature;

deriving a portion of a second network address from the public key of the first computing device;

validating the digital signature by using the public key of the first computing device; and

caching the public key in association with the first network address if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from ~~at least one of~~ the content data and/or a hash value of data including the content data.

12. (Original) The method of claim 11, wherein the authentication information further includes a modifier, and wherein deriving includes appending the modifier to the public key of the first computing device before deriving a portion of the second network address.

13. (Original) The method of claim 11, further comprising:

determining whether to cache the public key in association with the first network address based on a time stamp in the authentication information.

14. (Original) The method of claim 11 further comprising:

comparing the first network address against a network address in a public key/network address association already in the cache; and

if the first network address matches the network address in the public key/network address association already in the cache, and if the public key does not match a public key of the public key/network address association already in

the cache, then discarding the public key and first network address without caching them.

15. (Original) The method of claim 14 further comprising:

if the first network address matches the network address in the public key/network address association already in the cache, and if the public key does not match a public key of the public key/network address association already in the cache, then removing from the cache the public key/network address association already in the cache.

16. (Original) The method of claim 11 further comprising:

associating a timer with the caching of the public key/network address association;

resetting the timer if a second public key/network address association, identical to the public key/network address association, is presented for caching; and

if the timer expires, removing the public key/network address association from the cache.

17. (Currently Amended) A computer-readable medium containing instructions for performing a method for a second computing device to maintain a cache of at least one public key/network address association, the method comprising:

accessing authentication information made available by a first computing device, the authentication information including content data, a public key of the first computing device, a first network address of the first computing device usable to route a message to the first computing device, and a digital signature;

deriving a portion of a second network address from the public key of the first computing device;

validating the digital signature by using the public key of the first computing device; and

caching the public key in association with the first network address if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from ~~at least one of~~ the content data and/or a hash value of data including the content data.

18-20. (Canceled)

21. (Currently Amended) A computer-readable medium having stored thereon a data structure, the data structure comprising:

a first data field containing data representing a public key of a computing device; and

a second data field containing data representing a network address of the computing device, the network address being derived at least in part from a hash of the public key and being usable to route a message to the first computing device.

22. (Original) The data structure of claim 21 further comprising:

a third data field containing data representing a time stamp.